

EXHIBIT
A

**THIS EXHIBIT HAS BEEN
REDACTED IN ITS ENTIRETY**

EXHIBIT B

NetStalkerTM
Installation and User's Guide



Version 1.0.2



Haystack Labs, Inc.

10713 RR 620 North, #521
Austin, TX 78726
512-918-3555
512-918-1265 FAX
5/96 NETSTALK

**THE NETSTALKER™ INSTALLATION AND USER'S GUIDE
DOCUMENT REVISION 1.0.2**

Copyright ©1996 Haystack Laboratories, Inc.

All Rights Reserved. Copying or reproduction without prior written approval is prohibited.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraphs (a) through (d) of the Commercial Computer Restricted Rights clause at FAR 52.227-19 when applicable, or in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software Clause at DFARS 252.227-7013, and in similar clauses in the NASA FAR Supplement. Contractor/ manufacturer is Haystack Laboratories, Inc., 10713 RR620 North, #521, Austin, TX 78726 (512) 918-3555.

Haystack Laboratories, Inc. (hereinafter "Haystack Labs") retains all ownership, copyright, patent, and other intellectual property rights to the *NetStalker* computer programs (hereinafter collectively called "*NetStalker*") and their documentation. Use of *NetStalker* is governed by the license agreement distributed with the original media. Your rights are detailed in your License Agreement, but include:

- The *NetStalker* source code is a confidential trade secret of Haystack Labs. You may not attempt to decipher or decompile *NetStalker* or develop source code for *NetStalker*, or knowingly allow others to do so.
- Only you and your employees and consultants who have agreed to the above restrictions may use *NetStalker* and only on the authorized equipment.
- Your right to copy *NetStalker* and this manual is limited by copyright law. Making copies, adaptations, or compilation works (except copies of *NetStalker* for archival purposes or as an essential step in the utilization of the program in conjunction with the equipment), without prior written authorization of Haystack Labs, is prohibited by law and constitutes a punishable violation of the law. Exporting software documentation to a foreign country is not permitted by Haystack Labs.

Haystack Labs provides this publication "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Haystack Labs may revise this publication from time to time without notice.

NetStalker is a trademark of Haystack Laboratories. BorderGuard and Security Router are registered trademarks of Network Systems Corp. All other trademarks are the property of their respective owners.

Portions of this software are copyrighted by the following organizations: Carnegie Mellon University and University of California-Berkeley.

NetStalker was created by: Steve Smaha, Steve Snapp, Jessica Winslow, Richard Letsinger, Crosby Marks, Charisse Castagnoli, Brita Womack, and Kristin Johnson.

Result: The router blocks the illegal access attempt. *NetStalker* sends an alarm to SSC system/network administrator. To monitor X-session requests, run the *NetStalker* configuration X-session_watch.

At this point, the system administrator at SSC has received multiple notifications from the attempted illegal accesses. He can now take corrective action to further secure his systems.

NSC Clients and How They Interface with *NetStalker*

Initial PCF filter configuration

NetStalker has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and *NetStalker*. The filters are created and downloaded to the router when you run the shell, INSTALL.filters. See Chapter 2 for information on installing *NetStalker*.

Receiving data from router Console redirect messages are sent by the NSC client to socket 1780. PCF crypto messages are received by *NetStalker* on socket 1781.

Controlling router

A Unix shell-accessible program turns on or turns off a router-based shunning response. A shunning response is an instruction to the router to reject all packets from a specified individual IP address. This shunning response is controlled from the *NetStalker* user interface. See Chapter 4 for information on creating a shunning response.

Securing the connection

Since the *NetStalker* server platform can be located anywhere on the network, there is the potential of an attacker manipulating the connection between the router and the *NetStalker* server platform.

The most efficient means of protecting this connection between the NSC router client and the *NetStalker* is to use separate BorderGuard routers between the *NetStalker* platform and the network, and then to configure an encrypted tunnel between the client router and the "guard" router that protects the *NetStalker* platform. Since all IP traffic between the *NetStalker* platform and client is encrypted on the network, the encryption provides confidentiality, integrity, and mutual authentication of the communicating parties.

Alternatively, the *NetStalker* platform can be located on an individual network segment that is directly connected to a dedicated port on the router it is monitoring.

EXHIBIT C

**THIS EXHIBIT HAS BEEN
REDACTED IN ITS ENTIRETY**

EXHIBIT D

**THIS EXHIBIT HAS BEEN
REDACTED IN ITS ENTIRETY**

EXHIBIT E

UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,
a California corporation

Plaintiff and
Counterclaim-Defendant,

vs.

CERTIFIED
COPY

Case No. 04-1199 (SLR)

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation; INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation; and SYMANTEC
CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs.

DEPOSITION OF GEORGE KESIDIS
VOLUME I

DATE: May 25, 2006

TIME: 9:13 a.m.

LOCATION: DAY CASEBEER MADRID &
BATCHELDER
20300 Stevens Creek Boulevard
Suite 400
Cupertino, CA 95014

REPORTED BY: KAREN L. BUCHANAN
CSR No. 10772

8696
21416

Bell & Myers

CERTIFIED SHORTHAND REPORTER, INC.

GEORGE KESIDIS, VOLUME I

MAY 25, 2006

1	Q. So let me ask the question again just very	17:46:50
2	simply, so we can make sure the record is clear. Can	17:46:54
3	events with the same source address reflect	17:46:59
4	underlying commonalities, correct?	17:47:01
5	A. Yes. I agree.	17:47:05
6	Q. Events with the same destination address	17:47:07
7	reflect commonalities, correct?	17:47:12
8	A. Yes.	17:47:19
9	Q. Events that are close in time reflect	17:47:22
10	underlying commonalities, correct?	17:47:26
11	A. Yeah.	17:47:30
12	Q. Can you give an example of integrating that	17:47:33
13	does not involve commonalities?	17:47:36
14	MR. POLLACK: Objection. Asked and answered.	17:47:37
15	THE WITNESS: Yeah, I -- you may integrate	17:47:44
16	different attacks that are part of a larger attack, so	17:47:53
17	there is a standard strategy of launching a decoy	17:48:00
18	attack prior to the launch of a primary attack, as I	17:48:05
19	previously described. And also with regard to a DDoS	17:48:14
20	attack, just to get off the worm example, what you're	17:48:17
21	looking for in a DDoS attack possibly is a dispersion	17:48:22
22	of destination addresses -- sorry, the source	17:48:24
23	addresses that are targeting a certain local	17:48:29
24	destination address. The commonality is the	17:48:33
25	destination address, but in fact, there is a	

UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,
a California corporation,

Plaintiff and
Counterclaim-Defendant,

vs.

CERTIFIED
COPY

CASE NO: 04-1199 (SLR)

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation; INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation; and SYMANTEC
CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs.

DEPOSITION OF GEORGE KESIDIS
VOLUME II

DATE: Friday, May 26, 2006
TIME: 9:00 A.M.
LOCATION: DAY, CASEBEER, MADRID &
BATCHELDER
20300 Stevens Creek Boulevard
Suite 400
Cupertino, CA 95014
REPORTER: Patricia Hope Sales, CRR
CSR License Number C-4423

8705
21418

Bell & Myers

CERTIFIED SHORTHAND REPORTER, INC.

GEORGE KESIDIS, VOLUME II

MAY 26, 2006

1	A. Okay.	11:50:49
2	Q. Okay. And I want to start with the -- the	11:50:49
3	preamble where it says, "a computer automated method of	11:50:49
4	hierarchical event-monitoring and analysis within an	11:50:49
5	enterprise network."	11:50:49
6	Was the prior art RealSecure system a -- did it	11:50:52
7	contain a method of hierarchical event-monitoring and	11:50:59
8	analysis in your opinion?	11:51:03
9	MR. POLLACK: Objection. Vague and ambiguous,	11:51:05
10	lacks foundation.	11:51:05
11	THE WITNESS: Hierarchical in the sense that	11:51:11
12	there was a -- a console that displayed groupings of	11:51:12
13	events from different sensors, I would agree.	11:51:19
14	BY MS. MOEHLMAN:	11:51:25
15	Q. And is it your opinion that the prior art	11:51:25
16	RealSecure system operated within an enterprise	11:51:28
17	network?	11:51:36
18	MR. POLLACK: Objection. Vague and ambiguous,	11:51:37
19	lacks foundation.	11:51:38
20	THE WITNESS: Generally I would agree.	11:51:45
21	BY MS. MOEHLMAN:	11:51:47
22	Q. Is it your opinion that in the prior art	11:51:47
23	RealSecure system, a plurality of RealSecure agents	11:51:51
24	were deployed in the enterprise network?	11:52:00
25	MR. POLLACK: Objection. Lacks foundation.	11:52:04

GEORGE KESIDIS, VOLUME II

MAY 26, 2006

1	A. The automatically receiving it?	11:55:03
2	The -- the kind of combination conducted by	11:55:21
3	ISS, that is to say, merely displaying the events at a	11:55:24
4	same console, is -- is not in my opinion what was meant	11:55:34
5	by "integration" in the claim.	11:55:51
6	So I -- I'm assuming that if simply displaying	11:56:08
7	the events as received is construed to be integrating,	11:56:17
8	then I would agree that the -- the "automatically"	11:56:29
9	element would be -- would be met, but I -- I didn't	11:56:36
10	really -- haven't really thought about it too	11:56:41
11	carefully.	11:56:43
12	Q. Is it your opinion that the RealSecure console	11:56:45
13	in the prior art merely displayed the events as	11:56:51
14	received?	11:56:55
15	MR. POLLACK: Objection. Lacks foundation,	11:56:57
16	vague and ambiguous.	11:56:58
17	THE WITNESS: I believe that for purposes of	11:57:03
18	brevity, that largely identical reports were -- were	11:57:06
19	grouped together for visualization purposes.	11:57:31
20	BY MS. MOEHLMAN:	11:57:43
21	Q. And by grouping them together, would you	11:57:43
22	consider that to be combining reports received?	11:57:46
23	MR. POLLACK: Objection. Vague and ambiguous.	11:57:52
24	THE WITNESS: Given a -- a plain meaning of the	11:57:57
25	word "combining," sure.	11:58:01

**EXHIBIT
F**

**THIS EXHIBIT HAS BEEN
REDACTED IN ITS ENTIRETY**